

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Microsoft xBox accounts associated with the gamertags  
and email addresses listed in Attachment A-1 that is  
stored at Microsoft Corporation USA

Case No. 3:22-mj-113

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-1

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

SEE ATTACHMENT C-1

Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig  
Applicant's signature

Andrea R. Kinzig, FBI Special Agent  
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
Telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 4/8/2022 @ 12:10 p.m.

City and state: Dayton, OH

Caroline H. Gentry  
United States Magistrate Judge



**ATTACHMENT A-1**

Information associated with the Microsoft xBox accounts associated with the gamertags of **Unorthodox#6545**, **Unorthodox2**, and **Angel#9057**, and/or any xBox accounts associated with the email addresses **larry.isaacjr777@gmail.com**, **larry.isaac1237@gmail.com**, and **larry.isaacjr3@gmail.com**, that is stored at premises controlled by Microsoft Corporation USA, a company that accepts service of legal process at 1 Microsoft Way, Redmond, Washington, 98052.

**ATTACHMENT B-1**  
**Particular Things to be Seized**

**I. Information to be disclosed by Microsoft Corporation USA (the “Provider”)**

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1 for the time period of January 1, 2021 to the present:

1. All account registration details, billing address, and all other records or information regarding the identification of the account, including full name, physical address, telephone numbers and other identifiers, the date and time when the account was created, the IP and MAC addresses used to register the account, the length of service, the types of service utilized, records of session times and durations, login IP and MAC addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
2. All billing information for the account, including billing address, payment instruments, and billing transaction history;
3. All IP logs and session details for the accounts;
4. All information regarding the gamertags for the account and associated account profile information;
5. All gamertag change history data, xBox online game history, and information about the user's access and use of xBox applications;
6. Serial numbers and other identification numbers for any related xBox consoles, computers, and cellular telephones;
7. All records related to any xBox contacts for the accounts;
8. All photos, videos, or other media files uploaded by the user;
9. The contents of all communications associated with the account, including stored or preserved copies of all voicemail messages, audio files, video files, text, text files, images, multimedia, chats, and instant messages (“IMs”) stored and presently contained in, or on behalf of, the account or identifier;

10. All privacy settings and other account settings, including privacy settings for individual activities, and all records showing which users have been blocked by the account;
11. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
12. For the accounts listed in Attachment A-1, all Microsoft accounts that are linked to any of the accounts listed in Attachment A-1 by cookies, creation IP address, recovery email address, and/or telephone number;

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459, or making the data available to the Federal Bureau of Investigation via the Provider's electronic portal.



## **II. Information to be seized by the government**

Items evidencing violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography), 18 U.S.C. §§ 2251(a) and (e) (production of child pornography), and 18 U.S.C. § 2422(b) (coercion and enticement) from January 1, 2021 to the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and production of child pornography and coercion and enticement.
2. Any images or videos depicting child pornography.
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any communications with minors, and any identifying information for these minors.
6. Any information related to the use of aliases.
7. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
8. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements.
9. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.
10. Any geo-location information for the account or other records reflective of the whereabouts of the account user.
11. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

**ATTACHMENT C-1**

<b><u>Code Section</u></b>	<b><u>Offense Description</u></b>
18 U.S.C. §§ 2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §§ 2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §§ 2252(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §§ 2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §§ 2251(a) and (e)	Production of Child Pornography
18 U.S.C. § 2422(b)	Coercion and Enticement

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS**

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

**INTRODUCTION**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A) and coercion and enticement (in violation of 18 U.S.C. § 2422). I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
2. Along with other agents, officers, and investigators of the FBI and Ohio Adult Parole Authority, I am currently involved in an investigation of child pornography and child exploitation offenses committed by LARRY ISAAC JR. (hereinafter referred to as "ISAAC"). This Affidavit is submitted in support of Applications for search warrants for the following:
  - a. Information associated with the Microsoft xBox accounts associated with the gamertags **Unorthedox#6545**, **Unorthedox2**, and **Angel#9057**, and/or any xBox accounts associated with the email addresses **larry.isaacjr777@gmail.com**, **larry.isaac1237@gmail.com**, and **larry.isaacjr3@gmail.com**, that is stored at premises controlled by Microsoft Corporation USA (as more fully described in Attachment A-1);
  - b. Information associated with the Google accounts associated with the email addresses **larry.isaacjr777@gmail.com**, **larry.isaac1237@gmail.com**, and **larry.isaacjr3@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-2); and
  - c. Information associated with the Facebook accounts associated with the vanity names of **larry.isaacjr.9** and **larry.isaac.7731234** and the user identification numbers of **100009483873312**, **100052284364780** and **100023148570220** that is stored at premises controlled by Facebook Inc. (as more fully described in Attachment A-3).
3. The purpose of the Applications is to search for and seize evidence of suspected violations of the following:

- a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) and 2252A(a)(5)(B) and (b)(2), which make it a crime to possess child pornography;
  - b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce;
  - c. 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce or attempt to produce child pornography; and
  - d. 18 U.S.C. § 2422(b), which makes it a crime to use a facility of interstate or foreign commerce to coerce and entice another individual to engage in illegal sexual activities or attempt to do so.
4. The items to be searched for and seized are described more particularly in Attachments B-1 through B-3 hereto and are incorporated by reference.
  5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
  6. This Affidavit is intended to show that there is sufficient probable cause to support the searches of the above noted accounts (as defined in Attachments A-1 through A-3). It does not contain every fact known to the investigation.
  7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), 2252A(a)(2) and (b)(1), 2251(a) and (e), and 2422(b) are present within the information associated with the above noted accounts (as described in Attachments A-1 through A-3).

#### **JURISDICTION**

8. This court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States” that “has jurisdiction over the offense being investigated” 18 U.S.C. § 2711(3)(A)(i).



**PERTINENT FEDERAL CRIMINAL STATUTES**

9. 18 U.S.C. §§ 2252(a)(2) and (b)(1) state that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
10. 18 U.S.C. §§ 2252A(a)(2) and (b)(1) state that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.
12. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) state that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
13. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual



depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

14. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.
  - a. For purposes of the statute, 18 U.S.C. § 2427 states that the term “sexual activity for which any person can be charged with a criminal offense” includes the production of child pornography, as defined in section 2256(8).
15. Ohio Revised Code Section § 2907.323(A)(1) (Illegal Use of a Minor in Nudity Oriented Material) states that it is a violation for any person to photograph any minor who is not the person’s child or ward in a state of nudity, or to create, direct, produce, or transfer any material or performance that shows the minor in a state of nudity.
16. Illinois code § 5/11-25 (Grooming) states that it is a violation for any person to knowingly use a computer online service, Internet service, local bulletin board service, or any other device capable of electronic data storage or transmission to seduce, solicit, lure, or entice, or attempt to seduce, solicit, lure, or entice, a child, a child’s guardian, or another person believed by the person to be a child or a child’s guardian, to commit any sex offense as defined in Section 2 of the Sex Offender Registration Act, to distribute photographs depicting the sex organs of the child, or to otherwise engage in any unlawful sexual conduct with a child or with another person believed by the person to be a child. As used in this Section, “child” means a person under 17 years of age.

## **BACKGROUND INFORMATION**

### **Definitions**

17. The following definitions apply to this Affidavit and Attachments B-1 through B-3 to this Affidavit:

- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. **“Child erotica”**, as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- f. **“Internet Service Providers”** or **“ISPs”** are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- g. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard.



Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- h. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- i. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- j. **“Uniform Resource Locator” or “Universal Resource Locator” or “URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- k. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.

#### xBox

- 18. The xBox network, formerly known as xBox Live, is an online multi-player gaming and digital media delivery service created and operated by Microsoft Corporation, a company based in Redmond, Washington. The xBox network is available on gaming system consoles

(including the xBox One and xBox 360 consoles), computers running the Windows operating system, cellular telephones, and tablets. The xBox network is available both as a free service and as a subscription-based service known as xBox Live Gold.

19. In order to use the xBox network, users need to create an xBox account. Creating an account includes entering an email address, password, and first and last name.
20. A gamertag is a player's username on the xBox network. A gamertag is a unique identifier that can include numbers, letters, and spaces. Gamertags can also contain avatar images.
21. xBox users can communicate with each other via voice and text chatting features. The text chatting feature is similar to other messenger applications, where users can exchange direct messages with other users. In these direct messages, users can exchange text and other media files such as images and videos.
22. The xBox network allows users to invite up to seven people to communicate online while watching movies or playing games. This feature is referred to as an xBox party.
23. Microsoft Corporation maintains various data on its servers related to the creation of Microsoft accounts and the use of the xBox network. This information includes the following:
  - a. Account Creation Data, including: (1) registration details (including information captured at the time of account creation), (2) billing information (which may include the address and payment instrument(s)), (3) billing transaction history, (4) IP logs (including IP addresses captured at the time of user logins), and (5) services utilized.
  - b. xBox Service Data, including: (1) registration details (including information captured at the time of account creations), (2) gamertag information (including gamertag change history), (3) serial number of related xBox consoles and other devices, (4) IP logs (including IP addresses captured at the time of the user login to the xBox services), (4) xBox contacts, (5) xBox online game history, and (6) stored communications (to include messages and media files exchanged with other users).

#### Google Services

24. Google LLC ("Google") is a multi-national corporation with its headquarters located in Mountain View, California. Google offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking



service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

25. In addition, Google offers an operating system ("OS") for mobile devices (including cellular phones) known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.
26. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. However, users can also sign up for Google accounts with third-party email addresses.
27. Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below. Google's services include but are not limited to the following:
  - a. Gmail: Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.
  - b. Contacts: Google provides address books for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.
  - c. Calendar: Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or



tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

- d. Messaging: Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.
- e. Google Drive: Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me". Google preserves files stored in Google Drive indefinitely, unless the user deletes them.
- f. Google Keep: Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to backup all the data from their device to Google Drive.

- g. Google Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.
- h. Google Maps: Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.
- i. Location History: Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.
- j. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy



access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

- k. Android Backup: Android device users can use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, call history, contacts, device settings, or SMS messages. Users can also opt-in through Google One to back up photos, videos, and multimedia sent using Messages
28. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.
29. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.
30. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.
31. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or

file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

32. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.
33. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.
34. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.
35. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).
36. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.
37. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and



experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

### Facebook

38. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.
39. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.
40. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.
41. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.
42. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular



dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

43. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.
44. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.
45. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.
46. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.
47. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.
48. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.
49. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.
50. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook

user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

51. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.
52. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.
53. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information



indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

54. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

### **FACTS SUPPORTING PROBABLE CAUSE**

#### **Background on ISAAC**

55. ISAAC is presently 24 years old. His date of birth is February 12, 1998.
56. Records from the Greene County, Ohio Common Pleas Court revealed that ISAAC was convicted in or around July 2018 of Gross Sexual Imposition Involving a Minor, in violation of Ohio Revised Code § 2907.05(A)(4) (pursuant to case 2018CR0088). ISAAC was sentenced to 24 months of imprisonment. As a result of this conviction, ISAAC is required to register as a Tier II sex offender (which requires registration for a period of 25 years).
57. In or around January 2020, ISAAC was released from his term of incarceration and began a term of parole. Pursuant to the terms of his parole, ISAAC was forbidden from having any unsupervised contact with minors and committing any criminal offenses. Also pursuant to the terms of his parole, officers of the Ohio Adult Parole Authority were authorized to search ISAAC's residence, personal belongings, and computer and electronic media at any time.
58. During the time period of November 2021 through February 2022, ISAAC reported to his parole officer that he resided at 580 Newport Road, Apartment 1A, in Xenia, Ohio. As part of his sex offender registration requirements, ISAAC also reported to the Greene County Sheriff's Office that he resided at this address. Officers of the Ohio Adult Parole Authority and the Greene County Sheriff's Office have verified that ISAAC resided at this address.

#### **Preliminary Information from Minor A**

59. On or around February 22, 2022, an adult male residing in Chicago, Illinois (who will be referred to for purposes of this Affidavit as "Adult Male A") contacted the Chicago Police Department to report a suspected sex offense involving a minor. Adult Male A reported that he had discovered that his 16-year old daughter (who will be referred to for purposes of this Affidavit as "Minor A") was having an online dating relationship with an individual named LARRY ISAAC. Based on the information Adult Male A learned from Minor A and Internet research, he believed that ISAAC was 24 years old and lived in Ohio.

60. On or around February 22, 2022, an officer from the Chicago Police Department spoke to Minor A at her residence about her relationship with ISAAC. In summary, Minor A provided the following information:
- a. Minor A met ISAAC online in November 2021. They developed a relationship and communicated with each other at least five times per day.
  - b. Minor A had told ISAAC that she was 16 years old.
  - c. During an exchange of text messages on or around January 18, 2022, ISAAC asked Minor A to send him pictures of her vagina on her cellular telephone. Minor A sent the pictures to ISAAC as requested. ISAAC did not send pictures of himself to Minor A.
61. Adult Male A also reported ISAAC's relationship with Minor A to the Greene County Sheriff's Department. This information was then disseminated to the Ohio Adult Parole Authority.
62. On or around February 23 and 24, 2022, an officer from the Ohio Adult Parole Authority contacted Adult Male A and Minor A via telephone. During these telephone calls, Minor A provided the following additional information about her relationship with ISAAC:
- a. Minor A had communicated with ISAAC via Facebook and xBox.
  - b. ISAAC's xBox gamertag was **Unorthodox#6545**, and Minor A's gamertag was **Angel#9057**. At one point during their communications, Minor A had provided the password to her xBox account to ISAAC.
  - c. ISAAC's Facebook profile name was "Larry Isaac Jr.", and Minor A's Facebook profile name was her true name.
  - d. Minor A provided the parole officer with the password for her xBox account. She also provided her consent for officers to search her account.
63. An attempt was made to interview Minor A in March 2022. Due to her emotional and mental state, the interview could not be completed at that time.

Violation of ISAAC's Parole

64. On or around February 23, 2022, officers of the Ohio Adult Parole Authority arrested ISAAC for violating the terms of his parole. Officers also collected and seized a Motorola cellular telephone and an xBox One gaming console from ISAAC's residence. Officers learned that the Motorola cellular telephone actually belonged to ISAAC's father, but that the father had given the device to ISAAC to use.



Searches of ISAAC's Electronic Devices

65. Pursuant to the terms of ISAAC's supervised release, the Motorola cellular telephone was examined. In summary, the following information was noted during a preliminary examination of the device:
- a. The cellular telephone number for the device was 937-559-7095.
  - b. Three email accounts that appeared to belong to ISAAC were established on the device: ***[larry.isaacjr777@gmail.com](mailto:larry.isaacjr777@gmail.com)***, ***[larry.isaac1237@gmail.com](mailto:larry.isaac1237@gmail.com)***, and ***[larry.isaacjr3@gmail.com](mailto:larry.isaacjr3@gmail.com)***. A fourth email account was also established on the device, but it appeared that this email account was used by ISAAC's father.
  - c. A Facebook account that appeared to belong to ISAAC's father was logged into on the device. However, there was another login established on the device for what appeared to be ISAAC's Facebook account – that being an account with a profile name of "Larry Isaacjr".
66. Also pursuant to the terms of ISAAC's supervised release, a preliminary manual review was conducted of ISAAC's xBox One console. It was noted that there were logins for three gamertags on this console: ***Unorthodox#6545*** (the gamertag that Minor A reported as being ISAAC's account), ***Unorthodox2***, and ***Angel#9057*** (the gamertag that Minor A reported as being her account). The ***Unorthodox#6545*** gamertag was associated with the email address ***[larry.isaacjr777@gmail.com](mailto:larry.isaacjr777@gmail.com)*** (which was one of the email accounts located on the Motorola cellular telephone). The ***Unorthodox2*** gamertag was associated with the email address ***[larry.isaac1237@gmail.com](mailto:larry.isaac1237@gmail.com)*** (which was another one of the email accounts located on the Motorola cellular telephone). The ***Angel#9057*** gamertag was associated with a Google email address containing Minor A's first and last names and four numbers.
- a. As noted above, Minor A reported that she had given the password for her xBox account to ISAAC. Given that her gamertag was set up as a login account on ISAAC's xBox console, it is reasonable to believe that ISAAC had logged into her account.
  - b. Based on my training and experience, I know that individuals involved in child exploitation offenses sometimes log into their minor victims' online accounts. These individuals do so for a number of reasons. One reason may be to monitor the victims' communications to ensure that they have not reported the relationships with the offenders to family members or friends. Another reason may be to gain access to more of the victims' photographs.
67. Pursuant to Minor A's consent, her ***Angel#9057*** xBox account was logged into and reviewed on ISAAC's xBox console. Communications exchanged between Minor A's



Angel#9057 account and ISAAC's Unorthodox#6545 account during the approximate time period of November 17, 2021 through February 23, 2022 were located<sup>1</sup>. In summary, the communications included the following:

- a. The communications began with ISAAC (using the gamertag of Unorthodox#6545) talking about how he was not able to play any games. It appeared based on the context of the communications that ISAAC and Minor A had already been communicating with each other before these initial communications.
- b. The communications continued on or around November 18, 2021 with ISAAC talking about how he could not maintain a stable relationship. ISAAC made a comment about wanting to harm himself. Minor A offered encouragement to ISAAC and expressed that she liked him. ISAAC expressed that he liked Minor A as well and said that he thought she would be "sexy fun to be with". Below are excerpts of these communications:

Minor A: I Think I kind of like you I know it's to soon to tell you about this and I'm sorry but what you were saying earlier it's been on my mind all day

ISAAC: Reallyy

Minor A: Yes

ISSAC: I um im surprised

Minor A: Why are you surprised you don't have to answer if you don't want

ISAAC: Your the frist to actually say anything like that to me

Minor A: Well I'm just being honest with you

ISAAC: Im going to be honest ill send to you

Minor A: One thing you should know about me I will always be honest with you

ISAAC: I like/love/whatever your funny goofy i bet your sexy fun to be with i don't know no1 in my life but you i will be honest loyal and i wont lie you probably heard this before but im tell im not lieing ill always be here for you even if you were dieing id be ans go ahead

Minor A: Actually I never had any one say theses things to me [emoticon]

- c. The communications continued on or around November 18, 2021 with ISAAC and Minor A expressing their love for each other. ISAAC asked Minor A to "prove" that she loved him. Minor A then sent ISAAC a clothed picture of herself, and ISAAC told her that she was "seexy" (presumably meaning "sexy"). Below are excerpts from these communications:

Minor A: Love you

---

<sup>1</sup> It was noted that the dates associated with the first few communications was not displayed. The first date displayed was November 17, 2021. Therefore, it appears that the communications began shortly before November 17, 2021.

ISAAC: Love you more  
 Minor A: No I love you more  
 ISSAC: Prove it  
 Minor A: How do you want me to prove it  
 ISAAC: Yin anyway you can  
 Minor A: *[Emoticons]*  
 ISSAC: You win i sent you a invite  
 Minor A: *Sends clothed image depicting Minor A*  
 Minor A: I don't like good in this photo  
 ISSAC: That you holy moly your actually seexy tho i likey

- i. Based on my training and experience, I believe that the above communications are consistent with offenders who are grooming children to eventually produce and send child pornography files.
- d. On or around November 20, 2021, ISAAC told Minor A that he was "wet" and that he wanted to see Minor A's "wetness" and "hornyness". Minor A proceeded to send ISAAC a picture with her shirt pulled up, exposing her nude breasts, and a close-up image of what appears to be her nude vagina. Below are excerpts from these communications:

ISAAC: I need some from you badly  
 Minor A: I'm a little kinky right now  
 ISSAC: Mmmm im west asf  
 ISAAC: I wish i could see your wetness  
 ISAAC: I cant hold it in  
 Minor A: I feel weird calling you sis specially because you're my girlfriend<sup>2</sup>  
 ISAAC: Yea me to  
 Minor A: Love you *[emoticons]*  
 ISSAC: Love you 2  
 ISAAC: *[Emoticons]*  
 Minor A: I am a little kinky because you said that  
 ISAAC: Mmmmm  
 ISAAC: Me so horny  
 ISAAC: I wish i can see your hornyness  
 ISAAC: When ever your ready  
 Minor A: *Sends image depicting a close-up of what appears to be Minor A's torso, with her shirt pulled up to expose her nude breasts*  
 Minor : *Sends image depicting a close-up of what appears to be Minor A's nude vagina*

- i. Based on my training and experience, I believe that the close-up image of Minor A's nude vagina depicts child pornography.

---

<sup>2</sup> Based on the context of various communications, it appears that ISAAC may be transgender.

- ii. Also based on my training and experience, I believe that ISAAC's requests of Minor A are consistent with an individual coercing and enticing a minor to produce child pornography.
- e. Throughout the communications that transpired during the approximate time period of November 2021 through February 2022, Minor A sent ISAAC a total of following (which includes the three images described above): approximately 18 images that depicted her face or her wearing clothing, approximately six images depicting her in states of nudity, and approximately 12 images depicting the lascivious display of her genitalia (i.e., child pornography). By way of example, three of the files depicting child pornography are described as follows:
  - i. On or around December 11, 2021, Minor A sent ISAAC an image depicting her completely nude and touching her vagina. She then sent another image that depicted her completely nude and using her fingers to spread apart her vagina. Before and after Minor A sent these two images, ISAAC stated the following: "I cant stop thinking about you on top of me wet and wild and yes im horny" . . . "Im dripping cum and wet asf".
  - ii. On or around January 17, 2022, Minor A sent ISAAC an image depicting a close-up of what appears to be her nude vagina, with her using her fingers to spread apart her vagina.
- f. In addition to the approximately 12 instances in which Minor A sent ISAAC child pornography files, there were other times in which it appeared that ISAAC was soliciting Minor A to produce additional child pornography. By way of example, below are excerpts from two of these communications:
  - i. On or around November 21, 2021, after Minor A sent ISAAC a picture of her face, ISAAC sent Minor A the following messages: "Love the pic" . . . "I miss you" . . . "A fingering video". In response to ISAAC's messages, Minor A sent ISAAC a picture of a patch that contained the words "BACK OFF!".
  - ii. On or around January 10, 2022, after Minor A sent ISAAC a picture of her face, ISAAC sent Minor A the following message: "Make sure you spread that pussy open wide". Minor A did not respond to this message.
- g. No communications were recovered in which ISAAC sent Minor A any images or videos depicting him.
- h. During the communications that transpired from approximately November 2021 through February 2022, ISAAC and Minor A continued to express their love for each other. They also talked about sexually explicit conduct that they wanted to engage in



with each other. There were a number of times when ISAAC told Minor A that he was horny. Furthermore, there were at least two occasions in which ISAAC told Minor A that he would kill himself if he ever lost her. Below are excerpts from some of these communications:

ISSAC: I love you so much if id lost you id kill myself

Minor A: You will never lose me

ISAAC: I hope i never will

Minor A: believe me you will never ever lose me

ISSAC: Promise

Minor A: Promise *[emoticons]*

.....

ISAAC: Babe I cant live without you I need you more than anything or anyone. I would eat that pussy till youu scream my name id chock you bite your neck give you a hecky then ill have suck mmy purple cock after you get done suckn it ima shove it in you and fuck your brains out then ill blind fold you and cuff you to the bed and put a gag in your mouth so you cant scream ima also cuff your legs to the bed as well so you cant really move then ima eat you raw after that your still cuffd to the bed ill

ISSAC: Switch my strap-on to a 10" put lube on it and destroy that pussy then after that ill lick your butt & fuck you in the butt then ill uncuff you let you eat me out and finger me then fuck me till i scream your name and i want you to chock me after that i want all 10" in my butt.after we are done we sleep naked and ill hold you in my arms and in the morning your going to wake up to me given you head. That my lovely wife is what i want to do babe im not to hurt you ill never hurt you .....

ISAAC: With you ill even die for you ill kill anyone over you if i have destroy the to make sure your ok then so be i don't want you to be hurt fuck taylor fuck everyone else who hurts you they got to get through me and they cant get through me anyway cuz ill kill them in cold blood you are my baby,babygirl,queen,whore,wife ,love of my life,ect babe i love you lots don't forget that i love you alot *[emoticons]*

.....

ISSAC: I don't know what kind of letter you want so ill give you a love letter babe i miss you when yoour not home i miss you when you don't talk to me i miss you when your noot around i love you for who you are i love you for whaat you like the way you are ect but the question is me (ugly) i been bullyed raped beaten to death and was suicidal i don't know if annyl cares i love so much more than you could love me your like a girlfriend/friend/wife/babe/baby/babygirl /ect. I cant lose you if I do id killmyself

ISAAC: Babe i love you

Minor A: I love you so much  
Minor A: And you will never lose me  
.....  
ISAAC: Btw im a sex addict so like im addicted to sex  
.....  
ISAAC: I want to fuck you so bad i want to be deep inside you so bad  
.....  
ISSAC: Im horny asf r u

- i. Although the xBox communications did not include any specific communications about Minor A's age, there were a number of times when Minor A talked about her school – including discussions about being at school, missing school days, and being bullied by other students at her school. One of the pictures Minor A sent to ISAAC appeared to depict her in her school bathroom, and another picture appeared to depict her in a school-related uniform. In addition, there were times when Minor A talked about her parents and needing to get a ride from her mother. On one occasion, ISAAC questioned Minor A about what her mother said when she “came in”.
  - i. As noted above, Minor A reported to an officer from the Chicago Police Department that she had told ISAAC that she was 16 years old. Based on Minor A's statement, the photos that Minor A sent to ISAAC (which depict an apparent minor), and the communications noted above, there is probable cause to believe that ISAAC did in fact know that Minor A was a minor.
- j. There were a number of times in which Minor A asked ISAAC to invite her to xBox parties. There were various times after these and other communications where it appeared, based on the context of the communications, that ISAAC and Minor A had communicated with each other via other platforms – either via the xBox parties or other social media and messenger communications. Below are two examples where comments were made that appeared to be related to communications on other platforms:
  - i. On or around November 21, 2021, ISAAC told Minor A the following: “Mmmm im still thinking about last night”.
  - ii. On or around November 23, 2021, Minor A told ISAAC the following: “My Xbox has you muted and I can't unmute you”. ISAAC responded sometime thereafter by stating the following: “Im sorry i feel like i m making you do things you do thngs you don't wanna do”.
- k. No communications were located in which ISAAC specifically discussed the possibility of meeting Minor A in person. However, there were two occasions in which ISAAC provided Minor A with his address (that being 580 Newport Rd., Apt. 1A, Xenia, Ohio), and there were two occasions in which Minor A provided ISAAC

with her address. Based on the surrounding communications, it was not clear why they had exchanged addresses. Therefore, it appeared that the addresses were provided in response to communications that transpired on another platform(s). In addition, there was an instance in which ISAAC referenced the possibility of Minor A coming to his location. These communications included the following: “Ima stab your bro i don’t if he fellows you down here let follow you hes a dead man no ifs and but im tired of hearing him harassing you its over”.

- i. The address that ISAAC provided was the location where his parole officer knew that he resided and where he was arrested at on or around February 23, 2022. The address that Minor A provided was the address where Minor A is known to reside and where the officer of the Chicago Police Department met her on or around February 22, 2022.
- l. On one occasion, ISAAC provided Minor A with the telephone number of 937-559-7095.
  - i. This telephone number matches the telephone number of the Motorola cellular telephone that was collected from ISAAC’s residence.
  - ii. Based on this communication and other information detailed in the Affidavit, it appears that ISAAC and Minor A also communicated with each other via cellular telephone communications.
- m. On approximately three occasions, ISAAC provided Minor A with the email address ***larry.isaacjr777@gmail.com***. On one of the occasions, ISAAC also provided Minor A with what appeared to be three account names: “larryisaac777 or sallymarie777 or slycooper777”.
  - i. This email address matches one of the email accounts that was found on the Motorola cellular telephone that was collected from ISAAC’s residence.
  - ii. It has not been determined at this time to which platforms the three noted account names possibly relate. However, ISAAC’s tendering of these apparent account names and email addresses, along with other information detailed in the Affidavit, is indicative that ISAAC has utilized multiple social media platforms and personas.
- n. Consistent with the information provided by Minor A, there was an instance in which she provided ISAAC with her email address (which is associated with her xBox gamertag), the password to her xBox account, and another possible password.
- o. There were times when messages were displayed indicating that some of the communications between ISAAC and Minor A had been deleted.



- i. It is unknown at this time what those messages contained, why they were deleted, and who deleted them (i.e., whether Minor A or ISAAC deleted the files).
- 68. The **Unorthodox#6545** xBox account required a passcode to access it, and it was not searched. The **Unorthodox2** account was unlocked, and the account was manually reviewed on the xBox One console. It was noted that this account contained a profile name of "Sally Marie". It was further noted that the **Unorthodox2** account contained communications with Minor A's **Angel#9057** account during the approximate time period of January 27, 2022 through February 14, 2022. In summary, the communications included the following:
  - a. ISAAC and Minor A expressed their love for each other on a number of times throughout the communications.
  - b. No image or video files were contained in these communications.
  - c. There were occasions in which ISAAC and Minor A made comments indicating that they had communicated with each other via xBox parties.
  - d. On or around February 11, 2022, ISAAC told Minor A that his birthday was the following day. On or around February 12, 2022, Minor A wished ISAAC a happy birthday.
    - i. As noted above, ISAAC's date of birth is February 12, 1998.
- 69. Based on the communications recovered from the **Angel#9057** and **Unorthodox2** accounts, it is reasonable to believe that ISAAC communicated with Minor A via two xBox gamertags – that being **Unorthodox#6545** and **Unorthodox2**.

#### Review of Facebook Accounts

- 70. As noted above, Minor A reported that she had communicated with ISAAC via xBox and Facebook.
- 71. On or around February 24, 2022, and again on or around April 1, 2022, I searched publicly available information on the Facebook website for possible accounts utilized by ISAAC. I located the following four accounts:
  - a. A Facebook account with a profile name of "Larry Isaacjr" and a vanity name of **larry.isaacjr.9** was located at the URL of <https://www.facebook.com/larry.isaacjr.9>. The profile picture for the account depicted two of the characters from the movie Suicide Squad. The only available

profile information for the account was a notation that the Facebook user worked at “Pot Heads”. The home page for the account included a picture of a white male who appears to be ISAAC. The Friends list for the account included an account with a profile name of Minor A’s first and last name and ISAAC’s father’s account.

- b. A Facebook account with a profile name of “Larry Isaac Jr.” and a user identification number of **100052284364780** was located at the URL of <https://www.facebook.com/profile.php?id=100052284364780>. The profile picture for the account was the same picture as that contained on the **larry.isaacjr.9** account noted above. The publicly available profile information noted that the Facebook user lived in Xenia, Ohio. The Friends list for the account included ISAAC’s father’s account as well as the **larry.isaacjr.9** account, but it did not include Minor A’s account.
  - c. A Facebook account with a profile name of “Larry Isaacjr” and a user identification number of **100009483873312** was located at the URL of <https://www.facebook.com/profile.php?id=100009483873312>. The profile picture for the account was an image depicting an album cover for the Insane Posse band. The home page for the account included a picture of a white male who appears to be ISAAC. The publicly available profile information noted that the Facebook user lived in Xenia, Ohio. The Friends List for the account included 13 accounts, none of which were Minor A’s account or ISAAC’s father’s account.
  - d. A Facebook account with a profile name of “Larry Isaac Jr. (larry Isaac jr)” and a vanity name of **larry.isaac.773124** was located at the URL of <https://www.facebook.com/larry.isaac.773124>. The profile picture for the account depicted a white male who appears to be ISAAC. The publicly available profile information noted that the Facebook user lived in Xenia, Ohio.
72. I also searched publicly available information on the Facebook website for Minor A’s account. I located an account with a profile name of Minor A’s first and last name and a user identification number of **100023148570220**, located at the URL of <https://www.facebook.com/100023148570220>. One of ISAAC’s Facebook accounts – the Facebook account with a profile name of “Larry Isaacjr” and a vanity name of **larry.isaacjr.9** – was located on Minor A’s Friends List.

#### Conclusion Regarding Accounts

73. Based on all of the information detailed in the Affidavit, I submit that there is probable cause to believe the following:
- a. ISAAC is the user of the Microsoft xBox accounts associated with the gamertags of **Unorthodox#6545** and **Unorthodox2**, and Minor A is the user of the xBox account associated with the gamertag of **Angel#9057**.

- b. ISAAC is the user of the Google accounts associated with the email addresses **larry.isaacjr777@gmail.com**, **larry.isaac1237@gmail.com**, and **larry.isaacjr3@gmail.com**.
  - c. ISAAC is the user of the Facebook accounts associated with the vanity names of **larry.isaacjr.9** and **larry.isaac.7731234** and the user identification numbers of **100009483873312** and **100052284364780**, and Minor A is the user of the Facebook account with the user identification number of **100023148570220**.
74. There is also probable cause to believe that ISAAC has coerced and enticed Minor A to produce child pornography, and that he has received and possessed child pornography files depicting Minor A. There is also probable cause to believe that ISAAC coerced and enticed Minor A to engage in sexual activity in which he could be charged with criminal offenses – that being Grooming under the Illinois Code and Illegal Use of a Minor in Sexually Oriented Material under the Ohio Revised Code. Furthermore, there is probable cause to believe the following:
- a. ISAAC has utilized at least two xBox accounts – that being accounts with the gamertags of **Unorthodox#6546** and **Unorthodox2** – to communicate with Minor A, to coerce and entice her to produce child pornography, and to receive and possess child pornography files. Given all of the information detailed in the Affidavit (including information detailed below), it is reasonable to believe that ISAAC may have also utilized other xBox accounts associated with his email addresses to communicate with Minor A and/or other minors.
  - b. Minor A utilized the xBox account with the gamertag of **Angel#9057** to communicate with ISAAC and to send him child pornography files.
  - c. ISAAC has utilized at least one Facebook account – that being the account with the vanity name of **larry.isaacjr.9** – to communicate with Minor A. Given all of the information detailed in the Affidavit (including information detailed below), it is reasonable to believe that ISAAC may have also utilized his other Facebook accounts (that being the accounts with the vanity name of **larry.isaac.7731234** and the user identification numbers of **100009483873312** and **100052284364780**) to communicate with Minor A and/or other minors.
  - d. ISAAC has utilized at least two of his Google accounts – that being **larry.isaacjr777@gmail.com** and **larry.isaac1237@gmail.com** – to register his xBox accounts. Therefore, these accounts served as instrumentalities of ISAAC's child pornography and child exploitation offenses.



Evidence Available in Email and Social Media Accounts

75. In my experience, individuals often post information on their social media accounts about other electronic accounts that they utilize – including their email addresses, other social media accounts, messenger accounts, and gaming system account. This information may provide evidentiary value to child exploitation investigations in that they help in identifying other accounts utilized by the offenders in furtherance of their child exploitation activities.
76. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via email addresses, other social media accounts (including Facebook), messenger accounts, and gaming system account (including xBox). I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
77. Also in my experience, individuals involved in child exploitation schemes often utilize email addresses, other social media accounts (including Facebook), messenger accounts, and gaming system account (including xBox) as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
78. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including photo sharing services, cloud accounts, email addresses, other social media accounts (including Facebook), messenger accounts, and gaming system account (including xBox). Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.
79. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

80. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.
81. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers typically send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. These documents can be materially relevant to investigations of child pornography and child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.
82. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.
83. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

#### Evidence Sought in Other Google Accounts

84. As detailed above, there is probable cause to believe that ISAAC has three Google accounts associated with the email addresses ***[larry.isaacjr777@gmail.com](mailto:larry.isaacjr777@gmail.com)***, ***[larry.isaac1237@gmail.com](mailto:larry.isaac1237@gmail.com)***, and ***[larry.isaacjr3@gmail.com](mailto:larry.isaacjr3@gmail.com)***.
85. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.



86. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.
87. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.
88. As detailed above, Google Location History is an application in which Google utilizes various data such as cell site information and Wi-Fi routers to locate and geo-locate a cellular telephone device. Google collects and stores this data if the application is enabled by the user, either during the set-up of the device or through the device's settings.
89. Based on my training and experience, I know that location information from cellular telephones and Google accounts can be materially relevant in investigations involving child pornography and child exploitation offenses. This information provides evidence of the travels undertaken by the subject when meeting with possible victims. Data regarding the subjects' whereabouts as obtained from location information can corroborate statements made by the subjects and victims and provide evidence of the locations where the criminal activities took place.
90. In addition, location data regarding the subjects' daily and routine whereabouts, as obtained from Google Location History information and other location data (such as IP logs and cell site records), is often materially relevant in investigations of child pornography and child exploitation offenses. This information can help in identifying the locations of the subjects' primary residences, locations where they routinely frequent, and locations where they maintain their belongings (such as storage units). All of these locations may lead to the identification of the places where the computer devices used in furtherance of the crimes, as well as other evidence of the crimes, may be present. Information regarding the subjects' daily and routine whereabouts may also lead to the identification of co-conspirators and other victims.
91. Most Electronic Service Providers who maintain location information for accounts (including Google LLC) will not analyze the records to provide data specific to particular locations and activities. Furthermore, all locations relevant to the investigation may not be known at the time that the records are requested from and produced by the providers. For example, information obtained pursuant to additional interviews and/or records obtained pursuant to search warrants may lead to the identification of new victims and new criminal conduct. As such, location information is requested from the providers for the entire time



period relevant to the investigation. Only information relevant to the investigation of the child pornography and child exploitation offenses will be seized (as further detailed below in paragraph 94).

Conclusion Regarding Probable Cause


92. Based on all of the information detailed above, there is probable cause to believe that information associated with the following accounts may contain evidence of ISAAC's child pornography and child exploitation offenses:
- a. Microsoft xBox accounts associated with the gamertags of **Unorthodox#6545**, **Unorthodox2**, and **Angel#9057**, and/or any other xBox accounts associated with the email addresses ***[larry.isaacjr777@gmail.com](mailto:larry.isaacjr777@gmail.com)***, ***[larry.isaac1237@gmail.com](mailto:larry.isaac1237@gmail.com)***, and ***[larry.isaacjr3@gmail.com](mailto:larry.isaacjr3@gmail.com)***;
  - b. Google accounts associated with the email addresses ***[larry.isaacjr777@gmail.com](mailto:larry.isaacjr777@gmail.com)***, ***[larry.isaac1237@gmail.com](mailto:larry.isaac1237@gmail.com)***, and ***[larry.isaacjr3@gmail.com](mailto:larry.isaacjr3@gmail.com)***; and
  - c. Facebook accounts associated with the vanity names of ***[larry.isaacjr.9](#)*** and ***[larry.isaac.7731234](#)*** and the user identification numbers of ***[100009483873312](#)***, ***[100052284364780](#)*** and ***[100023148570220](#)***.
93. Preservation requests were served to Microsoft Corporation USA, Google LLC, and Facebook Inc. for the above noted accounts.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

94. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Microsoft Corporation USA, Google LLC, and Facebook Inc. to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 through B-3. Upon receipt of the information described in Section I of Attachments B-1 through B-3, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 through B-3.

**CONCLUSION**

95. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and/or property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located in the accounts described in Attachments A-1 through A-5, including the following offenses: 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), 2252A(a)(5)(B) and (b)(2), 2252(a)(2) and (b)(1), 2252A(a)(2) and (b)(1), 2251(a) and (e), and 2422(b).
96. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 through B-3.
97. Because the warrants for the accounts described in Attachments A-1 through A-3 will be served on Microsoft Corporation USA, Google LLC, and Facebook Inc., who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

  
Special Agent Andrea R. Kinzig  
Federal Bureau of Investigation

SUBSCRIBED and SWORN  
before me this 8th of April 2022

  
Caroline H. Gentry  
United States Magistrate Judge

